AO 106 (Rev. 04/10) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: Julia E. Barry 6/24/16

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
(Briefly describe the property to be search
Or identify the person by name and address)
PROPERTY KNOWN AS:
CELLULAR TELEPHONE MODEL G3 LG-D850
SERIAL NUMBER: 504KPRW623054
IN THE POSSESSION OF THE FEDERAL BUREAU OF
INVESTIGATION HEADQUARTERS, LOCATED AT:
3301 West Memorial Road
Oklahoma City, OK 73134

Case No: M-16-183-CG

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

CELLULAR TELEPHONE MODEL G3 LG D850, Serial Number 504KPRW623054, as further described in Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(a) and (d)	Enticement of a child and advertisement of child pornography;
18 U.S.C. § 2252A(a)(2)(A)	Receipt and distribution of child pornography;
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	Possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography;
18 U.S.C. § 2422(b)	Coercion and enticement.

The application is based on these facts:

See attached Affidavit of Special Agent Jonathan Clark, Federal Bureau of Investigation, Ardmore Resident Agency, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

JONATHAN CLARK
Special Agent
Federal Bureau of Investigation, Ardmore Resident Agency

Sworn to before me and signed in my presence.

Date: June 24, 2016

Judge's signature

City and State: Oklahoma City, Oklahoma

CHARLES B. GOODWIN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jonathan Clark, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent with the Federal Bureau of Investigation ("FBI") since 2008, and am currently assigned to the Ardmore Resident Agency of the Oklahoma City division. As a Special Agent with the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through new agent training at Quantico, Virginia, the Internet Crimes against Children training in Atlanta, Georgia and my everyday work conducting these types of investigations. I have received training in the area of child pornography, sextortion, and child exploitation, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256). Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and 2251(d) (enticement of a child and advertisement of child pornography); 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography); 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography); and 18 U.S.C. § 2422(b) (coercion and enticement), are located within the cellular telephone described as a **Model G3 LG-D850, Serial Number 504KPRW623054** ("SUBJECT PHONE"), located at the Federal Bureau of Investigation Office, in Oklahoma City, Oklahoma.

JC

3. The statements contained in this affidavit are based in part on information gathered from the service of a Federal search warrant; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of Grand Jury subpoenas; the results of surveillance conducted by law enforcement agents; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

RELEVANT STATUTES

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2251(a) and 2251(d) (Enticement of a Minor and Advertising Child Pornography); 18 U.S.C. § 2252A(a)(2)(A), (Receipt, Transportation, and Distribution of Child Pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2) (Possession and Access, or Attempted Access, with Intent to View Child Pornography), and 18 U.S.C. § 2422(b) (Coercion and Enticement).

a. 18 U.S.C. §§ 2251(a) and 2251(d) prohibits a person from knowingly conspiring to make, print or publish, or causing to be made, printed or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

c. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

d. 18 U.S.C. § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

5. On or about March 29, 2016, the Ardmore, Oklahoma, Police Department notified the Ardmore Office of the Oklahoma City Division of the FBI that the Ardmore Police had been

dispatched to a residence the night before, where they spoke with the parents of an 11-year-old female, Jane Doe ("JD1"). JD1's father told the Ardmore Police that JD1 was scared because of Facebook messages she had received via Facebook Messenger—an application that allows users to send messages to one another through internet-accessible computers or cell phones—from a person whom she believed was male. Ardmore police officers reviewed JD1's cell phone and saw messages from a sender named "Saul Frias" telling JD1 that if she did not have sex with his friends, he would send "the video" to all of her friends and everyone that he knew. JD1's father told one of the officers that the last thing Saul Frias sent JD1 was a video of JD1 in which she appeared naked, "play[ing] with herself."

6. On or about March 30, 2016, FBI agents interviewed JD1's father. At the interview, he provided the FBI with JD1's cell phone and gave his consent for agents to search the phone. JD1's father told the FBI that on March 28, 2016, he became aware of threatening Facebook Messenger communications to his 11-year-old daughter, JD1, from an unknown individual. The unknown individual, he explained, was threatening to send naked photos of JD1 to JD1's Facebook friends. JD1's father told agents that he had taken his daughter's phone, and confirmed that she had been receiving messages from the individual via the Facebook Messenger application. He then sent the unknown individual a message from JD1's phone informing him that he was JD1's father, and demanding that the individual stop sending messages to JD1. The unknown individual then sent a naked picture or video of JD1 to JD1's phone via Facebook Messenger, which JD1's father received. JD1's father contacted the Ardmore Police Department.

7. On or about March 30, 2016, FBI agents interviewed JD1. JD1 told the FBI that she had received a friend request from someone known as "Saul Frias" on Facebook in or about mid-

March 2016. Shortly after becoming friends, the user of the Saul Frias Facebook account requested that JD1 send nude pictures of herself. JD1 told the FBI that she does not personally know the person using the Facebook profile Saul Frias. When JDI sent sexually explicit pictures of her masturbating to the user of the Saul Frias Facebook account, the person using that profile threatened to send JD1's pictures to JD1's family and friends.

8. On or about April 8, 2016, a digital forensic examination was conducted on JD1's cellular phone. The FBI Agent who reviewed the evidence on the cellular phone advised me that the phone contained, among other things, a video of a nude female touching her genitalia. The female appeared to be JD1. The phone also contained Facebook Messenger data from Saul Frias.

9. On April 8, 2016, FBI agents compared the picture associated with the Facebook Messenger data from Saul Frias on JD1's phone to the profile pictures on Facebook's website associated with user name "Saul Frias." Agents discovered that many Facebook users went by "Saul Frias," but that only one profile—belonging to "saul.frias.14"—exhibited the same profile picture as that on the messages sent to JD1's phone. Agents also noticed that user saul.frias.14 resides in Ardmore, Oklahoma.

10. On April 25, 2016, the FBI obtained a Grand Jury subpoena and served the same to Facebook for subscriber information and registration IP address—a unique numerical address that is assigned to a specific Internet Service Provider—for the saul.frias.14 Facebook profile.

11. On or about May 2, 2016, the FBI received the Facebook subpoena results for the saul.frias.14 Facebook profile. The results showed that the account was created on February 27, 2016, from IP address 104.4.15.65, and that the registration email address was simonsantana59@gmail.com.

12. The FBI then discovered, via open source data, that AT&T Internet Services was the service provider for IP address 104.4.15.65. On or about May 3, 2016, the FBI obtained a Grand Jury subpoena and served the same to AT&T Internet Services, requesting the subscriber information for IP address 104.4.15.65 as of February 27, 2016.

13. On or about May 5, 2016, the FBI received the requested subpoena results from AT&T. The results revealed that the account was subscribed to Claudia Merino, who resides at 208 6th Avenue SE, Ardmore, Oklahoma.

14. That same day, the FBI received information from the Ardmore Police Department that an individual had broken into a residence in Ardmore, Oklahoma, conducted lewd acts with a minor female, Jane Doe 2 ("JD2"), and attempted to kidnap JD2, threatening to kill her if she did not go with him. JD2's brother ran for help, and the subject fled.

15. Later that day, the FBI and the Ardmore Police Department conducted a knock and talk at 208 6th Avenue SE, Ardmore, Oklahoma, and encountered a male who identified himself as Simon Molina-Santana in the back bedroom of the residence. An Ardmore officer took a photograph of Molina-Santana and texted it to JD2's mother, who showed the photograph to JD2 and her brother. JD2's mother informed the officer that JD2 and her brother had both identified Molina-Santana as the man who had broken into the above-referenced residence in Ardmore, Oklahoma, conducted lewd acts with JD2, and attempted to kidnap her. The officers arrested Molina-Santana, and seized a cellular telephone, the SUBJECT PHONE, from his person. Officers also found a hoodie in the back bedroom in which they encountered Molina-Santana that matched the description of clothing that the aforementioned subject was wearing at the time of the alleged assault on JD2.

16. On May 11, 2016, the FBI obtained a federal search warrant for the Facebook profile of saul.frias.14. On May 13, 2016, the FBI received the search results, which revealed that the user of the saul.frias.14 Facebook profile portrayed himself as "Saul Frias," a young male between the ages of 15 and 17. Between March 5, 2016, and April 11, 2016, "Saul Frias" had sexual conversations using Facebook Messenger with 14 individuals who identified themselves as between the ages of 11 and 17. Those conversations included the exchange of child pornography, the enticement of a minor child to produce pornography, and the solicitation of sex with a minor child. Two additional individuals, who did not declare their age, also exchanged messages with and exchanged photos and or/videos of child pornography with saul.frias.14. In some cases, the user of the saul.frias.14 Facebook profile sent a picture of an older male and/or of the older male's erect penis to an underage individual, and represented that he was Saul Frias's 28 year-old-friend, that he was the person whose penis was in the photo, and that he wanted to have sex with her/him. The picture of Saul Frias's older "friend" appears to be the same Simon Molina-Santana arrested by the Ardmore Police Department on May 5, 2016.

17. On May 19, 2016, the Ardmore Police Department provided the SUBJECT PHONE, seized upon Molina-Santana's arrest, to the FBI. It is now being stored in evidence at FBI Headquarters in Oklahoma City, Oklahoma, at the address specified in Attachment A to this affidavit.

18. Based upon this information, I believe that the aforementioned Facebook Messenger exchanges between JD1 and an unknown individual were sent and/or received by the user of the saul.frias.14 Facebook profile from 208 6TH Avenue SE, Ardmore, Oklahoma, or from other locations in Ardmore, Oklahoma, using either the SUBJECT PHONE, or another electronic device not yet discovered.

DEFINITIONS

19. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves,

legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. "Computer hardware," as used herein, consists of all equipment which can receive,

capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, routers, modems, and network equipment used to connect computers to the internet, cellular phones that can access the internet, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, modems used to access the internet, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks), routers and network hardware used to connect to the internet or to connect to a computer network of computers.

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware,

IC

software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. A "Host Name" is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet.

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital

subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

o. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

p. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

q. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but

IC

not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

r. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

s. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

t. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

u. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. Computers, cellular telephones that possess the ability to connect to the Internet or World Wide Web, and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers and cellular telephones that possess the ability to connect to the Internet or World Wide Web basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

21. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and cellular telephone with the ability to take digital pictures, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning that photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store large amounts of data (in excess of 500 gigabytes), which provides enough space to store thousands of high-resolution photographs. Video

camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

22. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact via modem can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

23. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The same is true with respect to cellular telephones that can access the Internet. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years as has the storage capacity on cellular phones. These drives and cell phones can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy

IC

it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Additionally, it is now extremely easy and common for an individual with a phone with a camera and Internet access to simply take a photo and immediately send that photo to storage locations or simply send the photo to other users of the internet.

24. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

25. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

26. As is the case with most digital technology, communications by way of computer or cellular phone can be saved or stored on the computer or phone used for these purposes. Storing this information can be intentional, e.g., by saving an e-mail as a file on the computer or cellular phone or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's or cellular phone user's Internet activities generally leave traces or "footprints" in the web cache and

IC

elsewhere on the computer or cellular phone and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers and cellular phones commonly require agents to download or copy information from the computers and cellular phones and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) and cellular phones can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems and cellular phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system and cellular phones is an exacting scientific

procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer and cellular phones evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a computer system and cellular phone, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all of the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

29. The search procedure of electronic data contained in cellular phones, computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems and cellular phones to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems and cellular phones, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers and cellular phones that may be

IC

partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination—such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such cellular phones, computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND ON FACEBOOK

30. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook also operates an application, Facebook Messenger, which allows Facebook users to exchange photos and messages with other Facebook users. The Facebook Messenger application can be utilized on any device that can access the internet—*viz.*, by computer or smart phone.

31. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email address, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

32. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

33. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust, for example, the types of notifications they receive from Facebook.

34. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user's profile page also includes a "wall," which is a space where the user and his or her "friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

35. Facebook allows users to upload photos and videos. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and ta link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

36. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also put comments on the Facebook profiles of other users or on their own profiles. In addition, Facebook has a chat feature that allows users to send and receive instant

IC

messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

37. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

38. In addition to the applications described above, Facebook also provides its users with access to many other functionalities and applications on the Facebook platform.

39. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall posting; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejecting "Friend" requests; comments; gifts; pokes; tags; and other information about the user's access and use of Facebook applications.

40. Facebook also retains Internet Protocol (IP) logs for a given user ID or IP address. These logs may contain information about the actions taken by the User ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that

user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

41. Social media providers and social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service, the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account information). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complains from other users. Social media providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Facebook stores its information on servers which are located in California. The information and data that is provided by the user is done so buy use of the internet using electronic media such as computers that access the internet or smart phones that access the internet. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other information.

42. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user

/C

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). Therefore, the computers of Facebook users are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

43. Facebook can be accessed via the Internet by use of a computer, or a cellular phone with Internet access/smart phone. Neither method is exclusive. Both methods can be used simultaneously and it is now commonplace for user to access Facebook by multiple methods.

44. In the FBI's experience and in the FBI's discussions with other law enforcement who conduct child exploitation investigations regarding Facebook, it is rare that a Facebook user uses only one method to use Facebook. It is more often the case that Facebook users use both computers and smart phones to access Facebook, as well as the Facebook Messenger Application. I believe that the SUBJECT PHONE is a smart phone and was used to access Facebook as well as to contact the victims described above in furtherance of the crimes outlined above.

CONCLUSION

45. Based on the foregoing, I believe that there is probable cause that the criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located on the SUBJECT PHONE, as described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PHONE, authorizing the search of the items described in Attachment B.

46. The FBI is aware that the recovery of data by a computer forensic analyst takes significant time; like narcotics, which must be forensically evaluated in a lab following, digital evidence must undergo a similar forensic process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

IC

Special Agent Jonathan Clark
Federal Bureau of Investigation

Sworn to me this 24th day of June, 2016.

The Honorable Charles B. Goodwin
United States Magistrate Judge

ATTACHMENT "A"

Description of Item to be Searched

The item to be searched is currently in the custody of the Federal Bureau of Investigation ("FBI"), identified as follows: **Cellular Telephone Model G3 LG-D850, Serial Number 504KPRW623054**, referred to as the "SUBJECT PHONE" in the Affadavit for Search Warrant. The item to be searched is currently located at the the FBI's Oklahoma City Headquarters, 3301 West Memorial Rd., Oklahoma City, OK 73134.

ATTACHMENT B

Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2422, 2251 and 2252A:

1. All data used as a means to commit the violations described above.
2. For the SUBJECT PHONE:
    a. evidence of who used, owned, or controlled the SUBJECT PHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the SUBJECT PHONE such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the SUBJECT PHONE was accessed or used to determine the chronological context of SUBJECT PHONE access, use, and events relating to crime under investigation and to the SUBJECT PHONE user;

e. evidence indicating the SUBJECT PHONE user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the SUBJECT PHONE of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT PHONE;

h. evidence of the times the SUBJECT PHONE was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT PHONE;

j. documentation and manuals that may be necessary to access the SUBJECT PHONE or to conduct a forensic examination of the SUBJECT PHONE;

k. records of or information about Internet Protocol addresses used by the SUBJECT PHONE;

l. records of or information about the SUBJECT PHONE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Text messages, e-mails, photographs to indivuals to entice minors to engage in sexually aexplicit conduct.
4. Child pornography and child erotica.
5. Text messages, e-mails, photographs sent via Facebook.
6. Records, information, and items relating to violations of the statutes described above including:
    a. Records, information, and items relating to the use or ownership of the SUBJECT PHONE, including utility and telephone bills paid or accessed by said SUBJECT PHONE, e-mails sent, accessed or received by SUBJECT PHONE, or Address and contact lists for text, e-mail, phone purposes;
    b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
    c. Records and information relating to the sexual exploitation of children, including correspondence and communications between users.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage for the SUBJECT PHONE.